NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

LISA BLACKMAN, *on behalf of herself individually and on behalf of all others similarly situated*, Plaintiff, v. **NORTHEAST SPINE & SPORTS MEDICINE, LLC**, Defendant.	Civil Action No. 24-7022 (ZNQ) (JTQ) **OPINION**

QURAISHI, District Judge

THIS MATTER comes before the Court upon a Motion to Dismiss pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) filed by Defendant Northeast Spine & Sports Medicine, LLC ("Defendant"). ("Motion," ECF No. 4.) Defendant filed a Brief in support of its Motion. ("Moving Br." at 4-1.) Plaintiff Lisa Blackman ("Plaintiff"), on behalf of herself and all others similarly situated ("the putative class"), filed a Brief in Opposition ("Opp'n Br.," ECF No. 8), to which Defendant replied. ("Reply Br.," ECF No. 9.) The Court has carefully considered the parties' submissions and decides the Motion without oral argument pursuant to Federal Rule of Civil Procedure 78 and Local Civil Rule 78.1.[1] For the reasons set forth below, the Court will **GRANT-IN-PART** and **DENY-IN-PART** the Motion.

[1] Hereinafter, all references to Rules refer to the Federal Rules of Civil Procedure unless otherwise noted.

I. BACKGROUND AND PROCEDURAL HISTORY

A. FACTUAL BACKGROUND[2]

Plaintiff brings this putative class action[3] against Defendant alleging negligence and breach of contract arising from a recent cyberattack and data breach. (Compl. ¶ 1, ECF No. 1-4.) Plaintiff seeks relief due to Defendant failing to (1) adequately protect Plaintiff's private information, (2) warn Plaintiff of its "inadequate" security practices, and (3) effectively secure hardware to protect Plaintiff's information. (*Id.* ¶ 12.)

Defendant is a "multi-specialty medical group in New Jersey specializing in orthopedic surgery, neurosurgery, pain management, sports medicine, chiropractic, physical [and] occupational therapy, acupuncture and massage." (*Id.* ¶ 2.) On or about January 15, 2024, Defendant was victim to a cyber-attack in which a ransomware group obtained the private information of Plaintiff and the putative class. (*Id.* ¶ 3.) The compromised information included personally identifiable information ("PII"), health insurance information, and medical treatment information, and is alleged to be in the hands of "cyber-criminals." (*Id.* ¶¶ 5, 6.)

The basis of the Complaint is that "Defendant failed to adequately protect Plaintiff's . . . Private Information—and failed to even encrypt or redact this highly sensitive information." (*Id.* ¶ 6.) As alleged, Plaintiff's information was compromised because of Defendant's "negligent and/or careless acts and omissions and its utter failure to protect patients' sensitive data." (*Id.* ¶ 9.) Plaintiff and the putative class have purportedly suffered injuries as a result of Defendant's negligent and reckless conduct. (*Id.* ¶ 11.)

---

[2] For the purposes of considering this Motion, the Court accepts all factual allegations in the Complaint as true. *See Phillips v. County of Allegheny*, 515 F.3d 224, 233 (3d Cir. 2008).

[3] The proposed class is defined as: "All persons in the United States whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach that occurred at Defendant in January 2024." (*See* Compl. ¶ 166.)

B. PROCEDURAL HISTORY

Plaintiff filed her initial Complaint on behalf of herself and all others similarly situated in the Superior Court of New Jersey on May 8, 2024. (*See* ECF No. 1-4; "Notice of Removal," ECF No. 1.) On June 11, 2024, Defendant timely removed the case to this Court. (Notice of Removal.) Thereafter, on July 1, 2024, Defendant filed the instant Motion to Dismiss. (ECF No. 4.)

II. SUBJECT MATTER JURISDICTION

The Court has original jurisdiction over this class action pursuant to the Class Acton Fairness Act ("CAFA"), 28 U.S.C. § 1332(d).[4]

While CAFA conveys subject matter jurisdiction, "[a]bsent Article III standing, a federal court does not have subject matter jurisdiction to address a plaintiff's claims, and they must be dismissed." *Taliaferro v. Darby Twp. Zoning Bd.*, 458 F.3d 181, 188 (3d Cir. 2006). The Court will therefore consider Plaintiff's Article III standing. *See In re Samsung Data Security Breach Litig.*, Civ. No. 23-3055, 2025 WL 26688, at *3 (D.N.J. Jan. 3, 2025) (noting that "[w]hen a plaintiff fails to establish Article III standing, the court lacks subject matter jurisdiction," and that "courts may dismiss a suit *sua sponte* for lack of subject matter jurisdiction at any stage" of the proceedings. (internal citations omitted)).

Article III of the United States Constitution confines the federal judicial power to the resolution of "Cases" and "Controversies." U.S. Const. Art. III. For there to be a case or controversy under Article III, the plaintiff must have a "'personal stake' in the case—in other words, standing." *TransUnion v. Ramirez*, 594 U.S. 413, 423 (2021) (quoting *Raines v. Byrd*, 521

[4] CAFA provides federal courts with original jurisdiction over civil class actions if the removing party establishes that the: (1) parties are minimally diverse; (2) proposed class has more than 100 members; and (3) "matter in controversy exceeds the sum or value of $5 [million] exclusive of interest and costs." *Judon v. Travelers Prop. Cas. Co. of Am.*, 773 F.3d 495, 500 (3d Cir. 2014) (quoting 28 U.S.C. § 1332(d)(2), (d)(6)). "To determine whether the[se] . . . jurisdictional requirements are satisfied, a court evaluates allegations in the complaint and . . . [the] notice of removal." *Id.* Having done so, the Court is satisfied that the elements of CAFA are met for purposes of jurisdiction.

U.S. 811, 820 (1997)). To have standing, a plaintiff must show, (1) that he or she suffered an injury in fact that is concrete, non-hypothetical, particularized, and actual or imminent; (2) that the injury was likely caused by the defendant; and (3) that the injury would likely be redressed by judicial relief. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). In order "[t]o establish [an] injury-in-fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339 (2016) (internal quotations omitted). "For an injury to be particularized, it must affect the plaintiff in a personal and individual way." *Id.* The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements as to each claim. *FW/PBS, Inc. v. Dallas*, 493 U.S. 215, 231 (1990).[5]

The Third Circuit has addressed standing in the specific context of data breaches. In *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011), the Circuit affirmed a district court's dismissal for lack of standing because the plaintiffs' contentions relied on "speculation that the hacker: (1) read, copied, and understood their personal information; (2) intend[ed] to commit future criminal acts by misusing the information; and (3) [was] able to use such information to the detriment of [the plaintiffs] by making unauthorized transactions in [the plaintiffs'] names." It added that "[u]nless and until these conjectures come true, [the plaintiffs] have not suffered any injury; there has been no misuse of the information, and thus, no harm." *Id.*

Years later, the Third Circuit held in *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155–56 (3d Cir. 2022), that "in the data breach context, where the asserted theory of injury is a substantial risk of identity theft or fraud, a plaintiff suing for damages can satisfy concreteness as long as he

[5] "In the context of a class action, Article III must be satisfied by at least one named plaintiff." *Neale v. Volvo Cars of N. Am.*, 794 F.3d 353, 359 (3d Cir. 2015); *see also O'Shea v. Littleton,* 414 U.S. 488, 494 (1974) ("[I]f none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class.").

alleges that the exposure to that substantial risk caused additional, currently felt concrete harms." It explained that "if the plaintiff's knowledge of the substantial risk of identity theft causes him to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury." *Id.* The *Clemens* Court explained that

> the injury must be "actual or imminent, not 'conjectural' or 'hypothetical.'" That "actual or imminent" is disjunctive is critical: it indicates that a plaintiff need not wait until he or she has actually sustained the feared harm in order to seek judicial redress, but can file suit when the risk of harm becomes imminent. This is especially important in the data breach context, where the disclosure of the data may cause future harm as opposed to currently felt harm. In this way, depending on the nature of the data at issue, claims flowing from a data breach can differ from traditional tort claims like defamation or invasion of privacy. While a claim arising from a data breach may share some commonalities with such torts—*e.g.*, in that it may involve the publication of information to a third party or unauthorized access to private information—the latter claims involve actual injury. A claim for defamation, for instance, rests on the "reputational harm" that flows from the publication of a statement "that would subject [the victim] to hatred, contempt, or ridicule." And a claim for invasion of privacy contemplates that the exposure "cause[s] mental suffering, shame or humiliation" to the victim. By contrast, the type of data involved in a data breach may be such that mere access and publication do not cause inherent harm to the victim. Even then, however, it can still poise the victim to endure the kind of future harm that qualifies as "imminent."

Id. at 152 (citations omitted). The Third Circuit expanded on these principles in a third decision in 2023, noting that "a plaintiff cannot establish an ongoing or imminent injury simply through allegations that an unknown hacker . . . potentially gained access to sensitive information in a large data breach." *Parker v. Governor of Pennsylvania*, Civ. No. 22-2789, 2023 WL 5814603, at *3 (3d Cir. Sept. 8, 2023), *cert. denied*, 144 S. Ct. 813 (2024).

Since *Clemens*, courts in this Circuit have analyzed standing in data breach cases using a three-factor non-dispositive test: (1) whether the data breach was intentional; (2) whether the data

was misused; and (3) whether the nature of the information accessed through the data breach could subject a plaintiff to a risk of identity theft (*i.e.*, disclosure of social security numbers, birth dates, and names—though, disclosure of financial information alone, without corresponding personal information, is insufficient). *Clemens*, 48 F.4th at 154; *see, e.g.*, *Alonzo v. Refresco Beverages US, Inc.*, Civ. No. 23-22695, 2024 WL 4349592, at *5 (D.N.J. Sept. 30, 2024).

Here, for the reasons set forth below, the Court finds that Plaintiff has standing. In relevant part, the Complaint alleges that Plaintiff (1) spent time mitigating the impact of the data breach (Compl. ¶ 156), (2) suffered actual injury (*id.* ¶ 157), including being victim to $45 in fraudulent charges, (*id.* ¶ 158), (3) received and continues to receive spam calls, (*id.* ¶ 159), and has anxiety, fear, and stress as a result of the data breach (*id.* ¶ 160.) These allegations are sufficient to confer Article III standing because they show that Plaintiff's data was misused and that she suffered concrete injuries. *See Clemens*, 48 F.4th at 155–56 (explaining that "if the plaintiff's knowledge of the substantial risk of identity theft causes him [or her] to presently experience emotional distress or spend money on mitigation measures like credit monitoring services, the plaintiff has alleged a concrete injury"). Moreover, the Court finds that the factors for standing established in *Clemens* for data breach cases likewise support a finding that Plaintiff has standing. Generally, cyber-attacks involve some degree of intentional conduct just by the very nature of the attack. *Alonzo*, 2024 WL 4349592, at *5. Here, the Complaint alleges that a ransomware group took credit for the cyberattack, thus showing that the attack involved some degree of intentional conduct. (Compl. ¶¶ 3, 31.) Considering (1) the intentionality of the attack, (2) that the data was misused, and (3) the type of data accessed, the Court finds that Plaintiff has Article III standing.

III. LEGAL STANDARD

Rule 8(a)(2) "requires only 'a short and plain statement of the claim showing that the pleader is entitled to relief,' in order to 'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests.'" *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) (alteration in original) (quoting *Conley v. Gibson*, 355 U.S. 41, 47 (1957) (abrogated on other grounds)).

A district court conducts a three-part analysis when considering a motion to dismiss pursuant to Rule 12(b)(6). *Malleus v. George*, 641 F.3d 560, 563 (3d Cir. 2011). "First, the court must 'tak[e] note of the elements a plaintiff must plead to state a claim.'" *Id.* (alteration in original) (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 675 (2009)). Second, the court must accept as true all of the plaintiff's well-pled factual allegations and "construe the complaint in the light most favorable to the plaintiff." *Fowler v. UPMC Shadyside*, 578 F.3d 203, 210 (3d Cir. 2009) (citation omitted). The court, however, may ignore legal conclusions or factually unsupported accusations that merely state the defendant unlawfully harmed the plaintiff. *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 555). Finally, the court must determine whether "the facts alleged in the complaint are sufficient to show that the plaintiff has a 'plausible claim for relief.'" *Fowler*, 578 F.3d at 211 (quoting *Iqbal*, 556 U.S. at 679). A facially plausible claim "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 210 (quoting *Iqbal*, 556 U.S. at 663). On a Rule 12(b)(6) motion, the "defendant bears the burden of showing that no claim has been presented." *Hedges v. United States*, 404 F.3d 744, 750 (3d Cir. 2005) (citing *Kehr Packages, Inc. v. Fidelcor, Inc.*, 926 F.2d 1406, 1409 (3d Cir. 1991)).

IV. DISCUSSION

Plaintiff asserts two causes of action in her Complaint: (1) negligence, (*id.* ¶¶ 181–218), and (2) breach of an implied contract, (*id.* ¶¶ 219–251).[6] The Court will address whether to dismiss each count in turn.

A. NEGLIGENCE

The Complaint alleges that Defendant had a duty to adopt reasonable measures to protect Plaintiff's private information, in light of the obligations arising from the Federal Trade Commission Act ("FTC Act") and the Health Insurance Portability and Accountability Act ("HIPAA"). (*Id.* ¶¶ 27–28.) Moreover, Plaintiff claims that Defendant did not use reasonable security procedures to protect Plaintiff's personal information from hackers. (*Id.* ¶ 33.) Plaintiff provides examples in the Complaint of ways in which Defendant was negligent and could have implemented more secure measures. (*See id.* ¶¶ 41, 42.) As a result of Defendant's negligence, the Complaint alleges that Plaintiff and the putative class suffered injuries "directly and proximately caused by Defendant's failure to implement or maintain adequate data security." (*Id.* ¶¶ 63, 116, 143–145, 148, 157, 159–160.)

Defendant argues that the Court should dismiss Plaintiff's negligence claim because the Complaint insufficiently alleges causation and damages. (*Id.* at 3.) Defendant claims that Plaintiff's allegations of damages are "vague and speculative . . . and do not support Plaintiff's

[6] In its briefs, Defendant notes the Complaint's passing references to the New Jersey Consumer Fraud Act ("NJCFA") and unjust enrichment. (Moving Br. at 18; Reply Br. at 13.) Defendant asks that these unasserted counts be dismissed as inadequately pled. Plaintiff maintains in opposition that she does state claims for fraud under the NJCFA and for unjust enrichment. (Opp'n Br. at 11–12.) The Court has reviewed the Complaint. There is no ambiguity; it clearly does not assert discrete counts for fraud under the NJCFA or for unjust enrichment. The Third Circuit has held that it is "axiomatic" that a plaintiff cannot amend her complaint in an opposition brief on a motion to dismiss. *Frederico v. Home Depot*, 507 F.3d 188, 202 (3d Cir. 2007). Accordingly, the Court will deny as moot Defendant's request to dismiss these unasserted claims.

claim of negligence." (*Id.* at 15–17.)[7] Plaintiff, however, insists that the Third Circuit has stated that injuries caused by a data breach are "easily and precisely compensable with a monetary award," and thus, Plaintiff has successfully pled damages. (Opp'n Br. at 7 (quoting *Clemens*, 48 F.4th at 158)). Plaintiff also refutes Defendant's claim that she did not suffer injuries arising from lost privacy rights, a diminished value of personal information, fraudulent charges, and lost time. (*Id.* at 8–11.)

To state a claim for negligence under New Jersey law, a plaintiff must assert that: (1) the defendant owed plaintiff a duty; (2) there was a breach of that duty; (3) the breach proximately caused the injury, and (4) damages. *Keith v. Truck Stops Corp. of Am.*, 909 F.2d 743, 745 (3d Cir. 1990); *Lax v. City of Atl. City*, Civ. No. 19-7036, 2019 WL 7207472, at *4 (D.N.J. Dec. 27, 2019). The question of whether a duty exists is a matter of law properly decided by the Court. *Strachan v. John F. Kennedy Memorial Hosp.*, 538 A.2d 346, 349 (N.J. 1988). Determination of the existence of a duty "is largely a question of fairness or policy." *Id.* "The inquiry involves a weighing of the relationship of the parties, the nature of the risk, and the public interest in the proposed solution." *V.C. by Costello v. Target Corp.*, 454 F. Supp. 3d 415, 423 (D.N.J. 2020).

Here, Plaintiff has thoroughly pled facts that state her claim for negligence. For example, she alleges that "Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep patients' Private Information safe and confidential." (Compl. ¶ 27.) Moreover, by "assuming the responsibility to collect and store this data . . . Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class

[7] Many of these arguments overlap with whether there is an injury-in-fact for Article III standing. The Court has already addressed Defendant's argument that Plaintiff's allegations of damages are too speculative.

Members' Private Information held within it—. . . from theft. (*Id.* ¶ 185.) That duty included "a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach." (*Id.*) Importantly, Plaintiff explains that "Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of being patients at Defendant." (*Id.* ¶ 190.)

Regarding breach, Plaintiff alleges that (1) Defendant had obligations created by the FTC Act and HIPAA, which it violated, (*id.* ¶¶ 28, 186, 187), (2) Defendant "failed to adequately protect Plaintiff's and Class Members' Private Information . . . [by] Defendant's negligent and/or careless acts and omissions and its utter failure to protect patients' sensitive data, (*id.* ¶ 6), and (3) "[i]t was foreseeable that Defendant's failure to use reasonable measures . . . would result in injury to Class Members." (*Id.* ¶ 203.) To support her claim that the breach of security was foreseeable, Plaintiff alleges that the "breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry." (*Id.*) The Complaint also provides examples of how Defendant could have protected Plaintiff's information, further supporting Plaintiff's claim for breach. (*Id.* ¶ 112). Lastly, the Complaint states that "Defendant failed to properly implement basic data security practices," (*id.* ¶ 95), and that Defendant failed to "employ reasonable and appropriate measures to protect against unauthorized access to its patients' Private Information," (*id.* ¶ 96).

In addition to properly alleging duty and breach, the Complaint alleges that "[b]ut for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private

Information of Plaintiff and the Class would not have been compromised," (*id.* ¶ 211), and that "[a]s a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses," (*id.* ¶ 214.)

Finally, with respect to damages, the Court finds that Plaintiff has sufficiently alleged facts to support relief as to past, present, and future harm for purposes of negligence. (*See, e.g.*, ¶¶ 156–160.) Defendant argues that the Court should dismiss Plaintiff's negligence claim because Plaintiff lacks standing to assert future damages given that such allegations represent future and speculative claims. (Moving Br. at 15, 22–23.) Plaintiff argues in opposition that the Court has standing for the "present and continuing threat of identity theft and fraud." (Opp'n Br. at 13–14.) Although it is true that an injury-in-fact for purposes of Article III standing must be imminent, materialized, and non-speculative, *see TransUnion*, 594 U.S. at 437 (noting that a "mere risk of future harm, without more" does not demonstrate Article III standing in a suit for damages), Defendant's argument seems to conflate the requirements of Article III standing and negligence.

In addition to the allegations directly resulting in injury-in-fact to Plaintiff, the Complaint alleges that "Plaintiff and [the] Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information." (Compl. ¶¶ 87, 143 ("Plaintiff and Class Members now face years of constant surveillance of their financial and personal records.")) Moreover, the Complaint alleges that "the risk of identity theft to the Plaintiff and the Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages." (*Id.* ¶ 116.) The Complaint also demonstrates that the type of PII that was stolen can lead to an imminent harm and alleges that

"Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions," which amounts to standing. (*Id.* ¶¶ 130–133.) Plaintiff moreover emphasizes the importance of social security number theft in the context of data breaches. (*See id.* ¶ 67). These allegations satisfy the requirements for pleading both Article III standing and the damages element of a negligence claim at this stage of the proceedings.

In short, the Court finds that the Complaint alleges a plausible claim for negligence. Accordingly, Defendant's Motion to Dismiss Plaintiff's negligence claim will be **DENIED**.

B. BREACH OF CONTRACT

The Complaint alleges that Defendant "made promises and representations to its patients that the private information collected from them as a condition of obtaining medical services . . . would be kept safe [and] confidential . . . and that Defendant would delete any sensitive information after they were no longer required to maintain it." (*Id.* ¶ 21.) That promise, however, was not kept in light of the data breach that took place. (*Id.*) Moreover, Plaintiff claims that there was a mutual understanding where Defendant would keep Plaintiff's information secure. (*Id.* ¶ 223.) And as a "direct and proximate result of Defendant's breach of the implied contract," the Complaint alleges that Plaintiff and the putative class sustained injuries and are entitled to damages. (*Id.* ¶¶ 236, 237.)

Defendant argues that the Court should dismiss Plaintiff's claim for breach of implied contract because the parties never entered into a contract, there are no reasonably definite terms alleged, there was no meeting of the minds, and there was no consideration. (Moving Br. at 1–2, 12–14.) Plaintiff maintains that she has properly pled mutual assent because there were express representations made in the privacy policies which are part of the course of conduct to create an implied contract. (Opp'n Br. at 1.) Plaintiff cites decisions from courts throughout the country

that have held that implied contracts were properly pled in similar data breach cases. (*Id.* at 5.) Plaintiff moreover suggests there is an implied contract because Plaintiff was required to give Defendant her personal information in order to obtain services provided by Defendant, and that in doing so, Plaintiff intended and understood Defendant would safeguard that information. (*Id.* at 7.)

To plead a claim for breach of contract under New Jersey law, a plaintiff must allege "(1) a contract; (2) a breach of that contract; (3) damages flowing therefrom; and (4) that the party performed its own contractual duties." *Video Pipeline, Inc. v. Buena Vista Home Entm't, Inc.*, 210 F. Supp. 2d 552, 561 (D.N.J. 2002); *Globe Motor Co. v. Igdalev*, 139 A.3d 57, 64 (N.J. 2016) ("Our law imposes on a plaintiff the burden to prove four elements: first, that '[t]he parties entered into a contract containing certain terms'; second, that 'plaintiff[s] did what the contract required [them] to do'; third, that 'defendant[s] did not do what the contract required [them] to do[,]' defined as a 'breach of the contract'; and fourth, that 'defendant[s'] breach, or failure to do what the contract required, caused a loss to the plaintiff[s]'" (quoting N.J. Model Civil Instr. 4.10A (May 1998))). Moreover, an enforceable contract may occur once a party communicates an offer and another party demonstrates acceptance. *Gordon v. Dailey*, Civ. No. 14-7495, 2018 WL 1509080, at *8 (D.N.J. Mar. 27, 2018). Importantly, acceptance may be shown by words or conduct. *See, e.g.*, *Weichert Co. Realtors v. Ryan*, 608 A.2d 280, 284 (N.J. 1992) ("An offeree may manifest assent to the terms of an offer through words, creating an express contract, or by conduct, creating a contract implied-in-fact"); N.J. Model Civil Instr. 4.10C.

Implied-in-fact contracts "are formed by conditions manifested by words and inferred from circumstances, thus entailing consideration of factors such as oral representations, employee manuals, and party conduct." *Iliadis v. Wal-Mart Stores, Inc.*, 922 A.2d 710, 722 (N.J. 2007). To

form an implied contract, a plaintiff must demonstrate "mutual assent" of the parties. *See In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, Civ. No. 19-2904, 2021 WL 5937742, at *19 (D.N.J. Dec. 16, 2021) ("Mutual assent is an essential element of an implied contract claim . . . .").

In the context of data breaches, however, "the fact that a defendant required plaintiffs to provide personal information does not alone support the inference that the parties agreed for the defendant to secure this information." *Id.* Rather, a complaint "must allege some other conduct by the Defendant from which mutual assent for [the defendant] to safeguard Plaintiff's PII arose." *In re Am. Fin. Res., Inc.*, 2023 WL 3963804, at *8; *see Longenecker-Wells v. Benecard Services Inc.*, 658 F. App'x 659, 662 (3d Cir. 2016) (explaining that plaintiffs, who were required to provide PII to their employer as a condition of employment, failed to plead an implied contract where the plaintiffs "failed to plead any facts supporting their contention that an implied contract arose between the parties other than that [Defendant] required Plaintiffs' personal information as a prerequisite to employment"); *see also Brush v. Miami Beach Healthcare Group Ltd.*, 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017) (similarly holding that "[n]othing in the Plaintiff's Complaint g[ave] rise to a factual inference that the [d]efendants tacitly agreed to secure her personal data in exchange for remuneration. It is clear from the Plaintiff's allegations that she transacted to receive healthcare services from the [d]efendants—not data security services beyond the privacy requirements already imposed on the [d]efendants by federal law. Accordingly, the Court cannot imply a contract to provide data security services based on the conduct of the parties.").

The Court finds that the Complaint fails to sufficiently plead breach of an implied contract. It is apparent from the Complaint that Plaintiff paid Defendants to perform medical services and she provided her PII as a pre-requisite to receiving Defendant's services. This is similar to the

plaintiff in *In re Am. Med. Collection Agency, Inc.*, where the court held the complaint failed to plead an implied contract. 2021 WL 5937742, at *19. Importantly, and fatal to surviving the Motion, is that Plaintiff fails to allege sufficient facts regarding the parties' mutual assent. The Complaint does not allege that Defendant agreed to safeguard the PII beyond complying with federal regulations. *See id.* Moreover, although the privacy notices on Defendant's website conveyed that Defendant was "sensitive to protecting [Plaintiff's] privacy," the website did not indicate that a contract existed or that Defendant was going to do something to protect that information. (*See id.* *22.)

Instead, the Complaint alleges that "Plaintiff and Class Members were required [to] deliver their Private Information to Defendant as part of the process of becoming patients at Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services." (*Id.* ¶ 220.) The Complaint further states that "Plaintiff . . . accepted Defendant's offers [to provide private information] . . . and provided their Private Information to Defendant," thereby accepting the offer. (*Id.* ¶ 221.)

These allegations do not suffice to plead that terms were agreed upon or that there was mutual assent. There also does not seem to be an offer regarding the PII. Rather, the underlying offer seems to refer to health services offered by Defendant. (*See id.* ¶ 2.) The Complaint adds that

> Plaintiff and the Class entrusted their Private Information to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

(*Id.* ¶ 223). Even construing the Complaint in a light most favorable to Plaintiff, these allegations fail to support a claim for breach of an implied contract because they do not adequately plead that

there was mutual assent.[8] And as stated, in the context of data breaches, "the fact that a defendant require[s] plaintiffs to provide personal information does not alone support the inference that the parties agreed for the defendant to secure this information." *In re Am. Med. Collection Agency, Inc.*, 2021 WL 5937742, at *19.

The Complaint attempts to allege that there was an implied-in-fact contract evidenced by Defendant's conduct. (*See id.* ¶ 226 ("[t]he mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.")). However, the allegations as to Defendant's conduct, even when liberally construed, do not plead a plausible basis to infer Defendant's assent. For example, the Complaint provides:

> On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

(*Id.* ¶ 227.) This allegation of an express promise is inconsistent with Plaintiff's claim for breach of *implied* contract. It is also conclusory because while it states that Defendants "expressly promised" that it would keep Plaintiff's information private, it asserts no facts to support that such an express agreement exists. The Complaint also alleges that "[o]n information and belief,

[8] The Complaint alleges that "[o]n information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach. (*Id.* ¶ 227.) This allegation is conclusory and does not adequately plead facts to support a finding that a policy existed. Moreover, this allegation is different from the allegations in *In re Am. Fin. Res., Inc. Data Breach Litig.*, Civ. No. 22-01757, 2023 WL 3963804, at *8–9 (D.N.J. Mar. 29, 2023), where the court held that the plaintiff adequately pled breach of an implied contract. In that case, the complaint provided that the defendant's website stated "[social security numbers] are classified as 'Confidential' information under the [defendant's] Information Security Policy . . . [and] are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information." *Id.* Here, Plaintiff makes no such allegation that there was a promise that the information will be stored and that procedural safeguards existed; being sensitive to private information, as alleged, does not demonstrate there was a promise or offer that was accepted.

Defendant further promised to comply with industry standards and to make sure that Plaintiffs and Class Members' Private Information would remain protected." (*Id.* ¶ 228). However, as set forth above, a promise to comply with industry standards does not create an implied-in-fact contract with Plaintiff.

Thus, because the Complaint does not plead the existence of mutual assent, the Court will **GRANT** the portion of the Motion seeking to dismiss Plaintiff's claim for breach of an implied contract. Plaintiff's breach of contract claim will therefore be dismissed without prejudice, and Plaintiff will be given leave to amend her Complaint.

V. CONCLUSION

For the reasons stated above, the Court will **GRANT-IN-PART** and **DENY-IN-PART** Defendant's Motion. (ECF No. 4.) Plaintiff will be given thirty days to amend its Complaint. An appropriate Order will follow.

Date: January 13, 2025

s/ Zahid N. Quraishi
ZAHID N. QURAISHI
UNITED STATES DISTRICT JUDGE